Assurance Cases Overview

Howard Lipson, CERT [vita[1]]

2007-1-4

Assurance Cases (AC) is a new content area for the knowledge category of the Build Security In (BSI) Web site. Our objective is to raise awareness about emerging methods and tools for assuring security properties of systems. In this content area, we introduce the concepts and benefits of developing and maintaining assurance cases for security. In particular, we describe the benefits of integrating assurance cases for security into the software development life cycle (SDLC) by "building assurance in" from the outset.

Elsewhere on the BSI Web site, the reader can learn about best practices, tools, and techniques that can help developers build security into their software. But the mere existence or claimed use of one or more of these best practices, tools, or techniques does not constitute an adequate assurance case. For example, in support of an overarching security claim (e.g., that a system is acceptably secure), security assurance cases must provide evidence that particular best practices, tools, and techniques were properly applied and must indicate by whom they were applied and their extent of coverage. Moreover, unlike many product certifications that quickly grow stale because they are merely snapshots in time of an infrequently applied certification process, a security assurance case should provide evidence that the practices, tools, or techniques being used to improve security were actually applied to the currently released version of the software (or that the results were invariant to any of the code changes that subsequently occurred).

A security assurance case uses a structured set of arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security properties. The case should be amenable to review by a wide variety of stakeholders. Although tool support is available, the creation and documentation of a security case can be a demanding and time-consuming process. Yet, similarities may exist among different security cases in the structure and other characteristics of the claims, arguments, and evidence used to construct the cases. A catalog of patterns (i.e., templates) for security assurance cases can facilitate the process of creating and documenting an individual case. Moreover, assurance case patterns offer the benefits of reuse and repeatability of process, as well as providing some notion of coverage or completeness of the evidence.

Articles in this Content Area

This is the first release of material for this content area. We expect that new documents will be added over time and that the existing material will continue to evolve. The initial document in this content area is described below.

- Arguing Security – Creating Security Assurance Cases[2]
  This introductory document describes the basic concepts associated with assurance cases and how they can be applied in the security domain (where they are known as *security cases*). What are security cases? What do security cases look like (i.e., what is their structure)? Why are they useful? When developing security cases it is common for arguments with the same structure to appear in many different contexts. A *security case pattern* takes advantage of this structural similarity and can reduce the effort needed to develop a security case. We explore an example of a security case, and a

1. daisy:15 (Lipson, Howard F.)
2. daisy:643 (Arguing Security - Creating Security Assurance Cases)

security case pattern, expressed graphically in Goal Structuring Notation.

Future Plans

Our future plans for the Assurance Cases content area (assuming the availability of resources) include steadily moving the focus of the material from introductory articles in the knowledge category toward material that can help establish security assurance cases as a best practice. Upcoming articles will provide detailed guidance on the practical steps that managers and practitioners can take to analyze and improve each phase of their software development life cycle process by applying security assurance case tools and techniques. Tutorial-level material will provide guidance on specific aspects of constructing a security case, such as how to gather and evaluate evidence. The use of security cases to support governance and management will be further elaborated. Our goal will be to help the reader learn how to use security assurance cases as a best practice to progress from ad hoc approaches, such as the use of unstructured security checklists, to the development and use of structured, reviewable arguments, backed by evidence that can be gathered continually throughout the SDLC (including system operations) and that can serve as a basis for continuous security improvement. As always, feedback and technical contributions from the community are most welcome.

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

Fields

Name	Value
Copyright Holder	SEI

Fields

Name	Value
is-content-area-overview	true
Content Areas	Knowledge/Assurance Cases
SDLC Relevance	Cross-Cutting

1. http://www.sei.cmu.edu/about/legal-permissions.html

Workflow State	Publishable